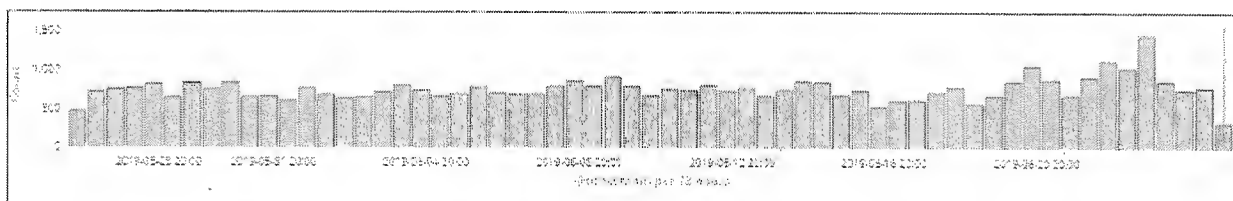


COMMONWEALTH OF PENNSYLVANIA)
)
) SS:
COUNTY OF YORK)

- I have been employed by CRIMEWATCH Technologies, Inc. (hereinafter sometimes “CRIMEWATCH”) as its Chief Technology Officer, for five (5) years.
- CRIMEWATCH was incorporated as a Pennsylvania Domestic Business Corporation in May of 2012 and has numerous competitors, including Neighbors App by RING (Amazon); NextDoor for Public Safety; Citizen App; Nixle by EverBridge; and possibly Harris Computer Systems who we believe is trying to create a competitive product.
- CRIMEWATCH does business in, or has planned business operations in, the States of Pennsylvania, Florida, New Jersey and Maryland and use of the CRIMEWATCH technology has been endorsed by the PA Chiefs of Police Association. The City of Harrisburg Police Department has been a customer of CRIMEWATCH for seven (7) years.
- CRIMEWATCH provides a uniform structured web portal, which standardizes where the public accesses public safety information and submits information to law enforcement. Law enforcement users can efficiently distribute information to multiple touch points with a single entry. The platform provides for real-time engagement with the public 24/7.
- CRIMEWATCH was specifically designed for law enforcement. CRIMEWATCH’s platform enables users to deliver the same narrative across multiple touch points, to include Media Outlets and Social Media (Facebook, Twitter) limiting /eliminating mis-information or “Fake news”. Law enforcement can control the who, what, when and where and can rebroadcast information as often as they like.
- CRIMEWATCH enhances Search Engine Optimization (SEO) of the information law enforcement pushes out, so that CRIMEWATCH data is found at or near the top of online searches. CRIMEWATCH’s ControlShare™ technology provides a “Chain of Custody” of the information you put out onto the Web so that it can easily be updated, edited or deleted across the web and social media even if it has been shared.
- I have a strong background in reverse engineering applications (5+ years as a Senior Research Engineer analyzing applications for various Anti-Malware companies), and training and documentation around any software product wherever available is the first place to start looking for potential exploits around the inner workings of the user interfaces, and to glean details of how the product works.

- CRIMEWATCH training manuals are all embedded and integrated directly into the CRIMEWATCH technology platform and releasing these would disclose proprietary design and function of the CRIMEWATCH platform. To clarify, there are no hard copies of any CRIMEWATCH training or user manuals; users can only get quick reference cards with paid access to the entire platform itself, but those quick reference cards would have screenshots and URL/Web Addresses containing sensitive customer-only URLs. However, the Agency in this case does not have access to any quick reference cards.
- CRIMEWATCH training and user materials are solely for our paying customers and would contain screenshots including URL/Web Addresses. Releasing these materials to the public would expose sensitive customer-only URLs throughout the CRIMEWATCH Network.
- These materials would be exposing our highly customized content types, workflows, and processes to competitors giving them sensitive insights into how they could potentially clone our highly matured and refined Software as a Service.
- Our trademarked ControlShare(tm) technology is also emphasized throughout these materials, putting a key proprietary feature of our products at risk of reverse engineering or cloning by competitors.
- There is otherwise no use or value in these materials for general public consumption as they cannot access any of the interfaces detailed within; releasing these materials would only be damaging to the company going forward.
- Domestic and foreign hackers are probing CRIMEWATCH constantly looking for holes in our security layers. We reactively and proactively block them as part of our day to day operations. Arming them with details as to how to curate and pull together content on our government/Law Enforcement customer portals means they now know which fields are required when creating various content types. This would help attackers, who are very much interested in finding vulnerabilities allowing them to both post content on CRIMEWATCH but also syndicate it out to the widest audience possible on behalf of the government entity – a key piece of functionality of what CRIMEWATCH does at its core.

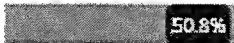
(see screenshots below illustrating the consistency and volume of blocked attempts to access content creation URLs on the CRIMEWATCH Network, over the past 1 month)



geoip.country_name

Top 5 values in 500 / 500 records

United States



Germany



Italy



United Kingdom



Brazil



In summary, disclosure of the CRIMEWATCH training material would expose critical details of the CRIMEWATCH infrastructure that would increase the likelihood of cyber-attack and potentially create catastrophic threats to the content delivery network which includes, the web, mobile, social applications and the private broadcast network of TVs. Only contracted police departments and authorized police department users, following CJIS (Criminal Justice Information Standards) with CLEAN certified are given access to these training tools and any corresponding documentation. All of this access is controlled through a POC at each department and is subject to regular audits. Each authorized user's activity is then monitored through a separate security application. The training program is provided through an access token to each authorized user and expires within 30 days. This access is monitored electronically as well. Every authorized user has to successfully complete the training program before they are granted full access to the platform. During this time, they can download quick reference cards, but this is done so with the expectation that they are not shared outside of the organization with non-authorized users. Being that our customers are police departments, integrity in these processes are of high importance as they are regulated throughout the organization.

Each employee at CRIMEWATCH has various degrees of understanding as it relates to the product and the proprietary interfaces that drive our system. Sales and marketing have an understanding to simply describe to a potential user how they will interact with the technology. The Customer Service team has a higher level of understand of the interfaces in how a customer best utilizes the system. Only the development team has full access to the proprietary nature of the engineering and processes happening throughout the system. These employees are subject to an inventions assignment and non-disclosure agreements, as are all employees of CRIMEWATCH.

If this information was shared and made public, it would be easy to duplicate the efforts that took nearly eleven years and more than 2 million dollars in research and development costs to create and implement. This disclosure would simply provide a roadmap of where to start when duplicating the system.


Mike Grucz
CTO, CRIMEWATCH Technologies, Inc.

Sworn to me this 28 day of
June, 2019


Notary Public

